

## DIGITAL WATERMARKING TECHNIQUES

MAYURI V. CHAUDHARI<sup>1</sup>, VARSHA R. POKHARKAR<sup>2</sup>, VRUSHALI CHOUDHARI<sup>3</sup> & LAVANYA RAO<sup>4</sup>

<sup>1,2</sup>Department of Electronics and Telecommunication, B. R. Harne College of Engineering, Thane, Maharashtra, India

<sup>3,4</sup>Department of Computer Engineering, B. R. Harne College of Engineering, Thane, Maharashtra, India

### ABSTRACT

Watermarking method has emerged in the 13<sup>th</sup> century which is a pattern or an image embedded on another image. Priorly watermark was impressed on a paper to show its authenticity. Watermark can be robust, fragile or semi-fragile. In this paper, we will see the methods of digital watermarking. Initially, the watermark is embedded on another image. Then noise is added before transmission which is then compressed and decompressed using suitable techniques such as JPEG compression technique. Finally, noise is removed and both the images are separated at the receiver side and the original image is obtained.

**KEYWORDS:** Types of Encryption, Digital Watermarking, Digital Watermarking, Classification of Watermarking, Methods

### INTRODUCTION

Network Security can be obtained using three techniques namely: cryptography, steganography and watermarking. In cryptography, original data is encrypted and then transmitted to the receiver. Hence, at the receiver the data is decrypted and the original data can be obtained. Steganography is used to hide data over any cover object and then transmitted to the receiver. Watermarking is a process used to hide information or data in digital media by using image, video or music files. The information which is embedded in a signal for transmission is known as a digital watermark. Watermarking is similar to steganography but the main difference both of them is that in watermarking the cover object is related to the hidden information. The signal for watermarking is called as host or base signal. Watermarking is done in three steps: embedding, attack and detection. In the first step, the data is embedded on the host signal and thus, a watermark signal is produced. This watermarked signal is then transmitted to the receiver. If the signal is modified during transmission then it is called as an attack. If the data is modified by any third party then attack is related to the copyright protection application.

### CLASSIFICATION

A signal may carry several watermarks but the size of the signal never changes. The signal can be obtained as it is if the signal is not modified. Thus, if the digital watermark is robust then the data can be retrieved as it is at the receiver. The embedded signal can be detected from the marked signal even if the signal is degraded. If the watermark is fragile then the extraction algorithm fails and the data at the receiver may change which means that the original data may be modified. The signal cannot be detected after modifications if the watermark is fragile. A semi-fragile digital watermark can resist benign transformations but the signal cannot be detected if the transformation is malignant. Hence, semi-fragile transformation is used to detect malignant transformations. When the marked signal is obtained by an additive modification then it is called as spread-spectrum water a mark. In quantization type digital watermarking the marked signal is obtained

by using quantization method. A digital watermarking is called as amplitude modification if the marked signal is embedded by additive modification.

## METHODS OF WATERMARKING

### Invisible Watermarking

Suppose an image 'X' is selected as a base image for transmission. Let another image 'Y' be the watermarked to be embedded. Now the least significant bit of image 'X' be replaced by most significant bit of watermark image 'Y'. As a result, image 'X' is watermarked with 'Y' and this new image be called as 'Z'. In this way, invisible watermarked is embedded in an image.

### Visible Watermarking-Concatenation

In concatenation method, suppose 'X' base image is selected and 'Y' is a watermark to be added then unlike invisible watermark the bits are not overwritten but both the images are concatenated to obtain a new image suppose 'Z'. As a result, a visible watermark is embedded in the image.

### Visible Watermarking-Noise Addition

This method is similar to concatenation method but in noise addition method noise is added to the image and it is further stored as a noisy image.

### Visible Watermarking-JPEG Compression

After the addition of noise JPEG compression is done which reduces the size of the file. After compressing the file, the file proceeds by removing the noise. The format of the watermarked that is added is converted to JPEG format.

### Visible Watermarking-Denoising and Separation of Images

In this, the noise added during in the file is removed and the watermarked image is obtained. Finally, both the images that is watermark and the original images are obtained and the data is retrieved as it is.

## CONCLUSIONS

Watermarking is an efficient method of hiding information. It is mainly used for copyright protection or authentication process. For this at the receiver end both the original and recovered images are compared and the data can be obtained.

## REFERENCES

1. Vidyasagar Potdar, Song Han, Elizabeth Chang, 'A survey of digital image watermarking techniques', *3<sup>rd</sup> IEEE International Conference on Industrial Informatics (INDIN 2005)*.
2. Ajinkya Kawale, Shubham Gaidhani, 'Digital Image Processing', *International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013*.
3. G.K. Wallace, 'The JPEG still picture compression standard', *IEEE Trans. On Consumer Electronics, vol.38, pp.18-34, Feb 1992*.
4. Rafael C. Gonzalez and Richard E. Woods 'Digital Image Processing'.